

# Maximum size of reverse-free sets of permutations \*

Josef Cibulka<sup>1</sup>

<sup>1</sup> Department of Applied Mathematics,  
Charles University, Faculty of Mathematics and Physics,  
Malostranské nám. 25, 118 00 Praha 1, Czech Republic;  
cibulka@kam.mff.cuni.cz

## Abstract

Two words have a reverse if they have the same pair of distinct letters on the same pair of positions in reversed order. A set of words no two of which have a reverse is said to be reverse-free. Let  $F(n, k)$  be the maximum size of a reverse-free set of words from  $[n]^k$  where no letter repeats within a word. We show the following lower and upper bounds in the case  $n \geq k$ :  $F(n, k) \in n^k k^{-k/2+O(k/\log k)}$ . As a consequence of the lower bound, a set of  $n$ -permutations each two having a reverse has size at most  $n^{n/2+O(n/\log n)}$ .

## 1 Introduction

Let  $[n]$  be the set of integers between 1 and  $n$ . A *word*  $w$  of length  $k$  over the alphabet  $A$  is a sequence  $w_1, \dots, w_k$  of elements from  $A$ . The set of all words of length  $k$  over  $[n]$  is  $[n]^k$ . A word is *repetition-free* if it contains at most one occurrence of each symbol. The set of all repetition-free words of length  $k$  over  $[n]$  is  $[n]_{(k)}$ . Notice that when  $n = k$ , the set  $[n]_{(n)}$  is the set  $S_n$  of permutations on  $n$  elements. A *code*  $\mathcal{F}$  of length  $k$  is a subset of  $[n]^k$ . The *size* of  $\mathcal{F}$  is the number of words in  $\mathcal{F}$ . Codes are usually defined to be sets of words that in some sense significantly differ from each other in order to be distinguishable when transmitted over a noisy channel. We study reverse-free codes introduced by Füredi, Kantor, Monti and Sinaimeri [7]. Two words  $w$  and  $x$  have a *reverse* if for some pair  $(i, j)$  of positions, we have  $w_i \neq w_j$ ,  $w_i = x_j$  and  $w_j = x_i$ . If  $w$  and  $x$  do not have a reverse, they are *reverse-free*. A code is *reverse-free* if its words are pairwise reverse-free. Let  $\overline{F}(n, k)$  be the size of the largest reverse-free code over  $[n]$  of length  $k$ . Let  $F(n, k)$  be the size of the largest reverse-free code over  $[n]$  of length  $k$  containing only repetition-free words. Let

$$f(k) \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} \frac{F(n, k)}{k! \binom{n}{k}}.$$

---

\*Research was supported by the grant SVV-2012-265313 (Discrete Methods and Algorithms) and by the Czech Science Foundation under the contract no. 201/09/H057.

The limit exists for every  $k \geq 1$  [7]. We will use the following equivalent definitions of the limit:

$$f(k) = \lim_{n \rightarrow \infty} \frac{F(n, k)}{n^k} = \lim_{n \rightarrow \infty} \frac{\overline{F}(n, k)}{n^k}.$$

The first equality follows from the fact that  $\lim_{n \rightarrow \infty} \binom{n}{k} k! n^{-k} = 1$ . The second equality is a consequence of the observation that for every fixed  $k$ , we have  $F(n, k) \leq \overline{F}(n, k) \leq F(n, k) + O(n^{k-1})$  [7]. The only exact values of the limit known are  $f(1) = 1$ ,  $f(2) = 1/2$  and  $f(3) = 5/24$  [7].

We tighten the bounds on the maximum size of reverse-free codes of length greater or equal to the size of the alphabet.

**Theorem 1.1.** *For every  $n \geq k$ , we have*

$$n^k k^{-k/2 - O(k/\log k)} \leq F(n, k) \leq \overline{F}(n, k) \leq n^k k^{-k/2 + O(k/\log k)}.$$

The first inequality is proven in Section 2 as Corollary 2.5 and the last inequality is proven as Claim 3.4 in Section 3. As an immediate consequence, we obtain the following bounds for permutation codes:

$$n^{n/2 - O(n/\log n)} \leq F(n, n) \leq \overline{F}(n, n) \leq n^{n/2 + O(n/\log n)}.$$

and for the limit for codes of fixed length  $k$ :

$$f(k) \in k^{-k/2 + O(k/\log k)}.$$

A set of words is *full of flips* if each two words from the set have a reverse. Let  $\overline{G}(n, k)$  be the size of the largest code full of flips with elements in  $[n]^k$ . Let  $G(n, k)$  be the size of the largest code full of flips with elements in  $[n]_{(k)}$ . By  $G(n, n)F(n, n) \leq n!$  [7], we obtain the following corollary.

**Corollary 1.2.** *The size of a set of permutations full of flips is at most*

$$G(n, n) \leq n^{n/2 + O(n/\log n)}.$$

A position of an entry of a matrix is represented by a pair  $(r, c)$  of the row number  $r$  and the column number  $c$ . A  $\{0, 1\}$ -matrix is a matrix whose each entry is either 0 or 1. Every matrix in this paper is a  $\{0, 1\}$ -matrix, even if not explicitly mentioned.

All logarithms in this paper are of base 2.

## 2 Lower Bound

A submatrix of a matrix  $B$  is a matrix that can be obtained from  $B$  by the removal of some columns and rows. An  $m \times n$   $\{0, 1\}$ -matrix  $B$  *contains* a  $k \times l$   $\{0, 1\}$ -matrix  $S$  if  $B$  has a  $k \times l$  submatrix  $T$  that can be obtained from  $S$  by changing some (possibly none) 0-entries to 1-entries. Otherwise  $B$  *avoids*  $S$ .

Füredi and Hajnal [6] studied the following problems from the extremal theory of  $\{0, 1\}$ -matrices. Given a matrix  $S$  (the *forbidden matrix*), what is the maximum number of 1-entries in an  $n \times n$  matrix that avoids  $S$ ?

We restrict our attention on forbidding the  $2 \times 2$  matrix with each entry equal to 1 and we call this matrix  $S$ . This question is closely related to the extremal problem of determining the maximum number of edges in an  $n$ -vertex graph without a 4-cycle as a subgraph. The maximum number of edges in a 4-cycle-free graph is known precisely for infinitely many values of  $n$  [5]. We will use a classical construction of a bipartite 4-cycle-free graph (see for example the book of Matoušek and Nešetřil [8]). We reproduce the construction here in the matrix setting since we need some of its additional properties.

The construction of a matrix avoiding  $S$  builds the matrix using a finite projective plane. Let  $X$  be a finite set and let  $\mathcal{L}$  be a family of subsets of  $X$ . The set system  $(X, \mathcal{L})$  is a *finite projective plane* if

(P0) There is a 4-tuple  $F$  of elements of  $X$  such that  $|F \cap L| \leq 2$  for every  $L \in \mathcal{L}$ .

(P1) For every  $L_1, L_2 \in \mathcal{L}$ ,  $|L_1 \cap L_2| = 1$ .

(P2) For every  $x, y \in X$  there exists exactly one  $L \in \mathcal{L}$  containing both  $x$  and  $y$ .

For every finite projective plane, we can find a number  $r$ , called the *order of the projective plane*, satisfying:

(P3) For every  $L \in \mathcal{L}$ ,  $|L| = r + 1$ .

(P4) Every  $x \in X$  is contained in exactly  $r + 1$  sets from  $\mathcal{L}$ .

(P5) We have  $|X| = |\mathcal{L}| = r^2 + r + 1$ . This value is the *size* of the projective plane.

It is known that for every number  $r$  that is a power of a prime number, we can find a finite projective plane of order  $r$  [8].

**Claim 2.1.** *If  $n$  is of the form  $r^2 + r + 1$ , where  $r$  is a power of a prime, then*

$$F(n, n) \geq n^{n/2 - O(n/\log n)}.$$

*Proof.* We fix a projective plane  $(X, \mathcal{L})$  of size  $n$ . We order the elements of  $X$  and the sets of  $\mathcal{L}$  arbitrarily. The *incidence matrix* of a finite projective plane of size  $n$  is the  $n \times n$  matrix  $A$  with 1 on position  $(i, j)$  exactly if the  $i$ -th set of  $\mathcal{L}$  contains the  $j$ -th element of  $X$ . Let  $A$  be the incidence matrix of  $(X, \mathcal{L})$ .

An  $n$ -*permutation matrix* is an  $n \times n$  matrix with exactly one 1-entry in every column and every row. An  $n$ -*permutation* is a permutation on  $n$  elements. The set of  $n$ -permutations and the set of  $n$ -permutation matrices are in the following bijection. The permutation  $\pi$  is matched with the matrix  $P$  with 1 on position  $(i, j)$  exactly if  $\pi_i = j$ . Let  $\mathcal{P}$  be the set of  $n$ -permutation matrices contained in  $A$  and let  $\Pi$  be the set of  $n$ -permutations matched to the matrices from  $\mathcal{P}$ . By (P3) and (P4),  $A$  has exactly  $r + 1$  1's in every row and every column. Thus by the van der Waerden conjecture proved independently by Falikman [4] and Egorychev [3],

$$|\Pi| = |\mathcal{P}| \geq \left(\frac{r+1}{n}\right)^n n! \geq \left(\frac{r+1}{e}\right)^n \geq \left(\frac{n^{1/2}}{e}\right)^n \geq n^{n/2 - O(n/\log n)}.$$

We claim that the set  $\Pi$  is pairwise reverse-free. For contradiction, we take  $\pi \in \Pi$  and  $\rho \in \Pi$  with a reverse on positions  $i$  and  $j$ . That is,  $\pi_i = k$ ,  $\pi_j = l$ ,  $\rho_i = l$ ,  $\rho_j = k$  for some  $k$  and  $l$ . Since  $P_\pi$  and  $P_\rho$  are contained in  $A$ , this implies that  $A$  contains the matrix  $S$  on rows  $i, j$  and columns  $k$  and  $l$ ; a contradiction with (P1).  $\square$

By the prime number theorem, the gaps between two consecutive prime numbers in proportion to the primes tend to zero. There has been a significant progress in tightening the gap between two consecutive primes. Most recent is the following result of Baker, Harman and Pintz [1].

**Theorem 2.2** (Baker, Harman, Pintz, 2001). *For every large enough  $n$ , the interval  $[n - n^{0.525}, n]$  contains a prime number.*

**Lemma 2.3.** *For every  $n$ ,*

$$F(n, n) \geq n^{n/2 - O(n/\log n)}.$$

*Proof.* For an arbitrary  $n$  we take the largest  $n'$  smaller than  $n$  and expressible as  $p^2 + p + 1$  for some prime  $p$ . We have

$$\begin{aligned} p &\geq n^{1/2} - 1 - n^{0.525/2} \quad \text{and so} \\ n' &\geq n - O(n^{1.525/2}). \end{aligned}$$

We take the set  $\Pi'$  of  $(n')^{n'/2 - O(n'/\log n')}$  pairwise reverse-free  $n'$ -permutations from Claim 2.1. We append the sequence  $(n' + 1, n' + 2, \dots, n)$  to the end of each  $\pi' \in \Pi'$ . Let the resulting set of  $n$ -permutations be  $\Pi$ . The set  $\Pi$  of permutations is pairwise reverse-free and has size at least  $n^{n/2 - O(n/\log n)}$ .  $\square$

**Lemma 2.4.** *For every  $n \geq k$ ,*

$$F(n, k) \geq \left\lfloor \frac{n}{k} \right\rfloor^k F(k, k).$$

*Proof.* Let  $\Pi$  be a reverse-free set of  $k$ -permutations of size  $F(k, k)$ . Given a word  $u = (u_1, u_2, \dots, u_k) \in [n]_{(k)}$ , we call the word  $(u_1 \bmod k, u_2 \bmod k, \dots, u_k \bmod k)$  the *compression* of  $u$ . Let  $\mathcal{F}$  be a set of all the words in  $[n]_{(k)}$  whose compression is in  $\Pi$ . The size of  $\mathcal{F}$  is at least  $\left\lfloor \frac{n}{k} \right\rfloor^k |\Pi|$ . It remains to show that  $\mathcal{F}$  is reverse-free. For contradiction, assume that some pair of words  $(u_1, \dots, u_k)$  and  $(v_1, \dots, v_k)$  has a reverse on the pair  $(i, j)$  of positions. That is,  $u_i = v_j$  and  $u_j = v_i$  and, in particular,  $u_i \bmod k = v_j \bmod k$  and  $u_j \bmod k = v_i \bmod k$ . Because the compression of  $u$  is a permutation,  $u_i \bmod k \neq u_j \bmod k$ . This is a contradiction, because the compressions of  $u$  and  $v$  are in the reverse-free set  $\Pi$ .  $\square$

**Corollary 2.5.** *For every  $n \geq k$ ,*

$$F(n, k) \geq n^k k^{-k/2 - O(k/\log k)}.$$

*Proof.* Since  $n \geq k$ , we have  $\lfloor n/k \rfloor \geq n/(2k)$ . Therefore, by Lemmas 2.3 and 2.4

$$F(n, k) \geq \left( \frac{n}{2k} \right)^k F(k, k) \geq \frac{n^k}{(2k)^k} k^{k/2 - O(k/\log k)} \geq n^k k^{-k/2 - O(k/\log k)}.$$

$\square$

### 3 Upper Bound

We adapt the classical proof of the  $O(n^{3/2})$  upper bound on the number of edges in a 4-cycle-free graph to show that a matrix with many 1-entries contains many occurrences of the matrix  $S = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ . That is, there are many pairs of rows and pairs of columns of  $A$  having 1's in their four intersections.

**Lemma 3.1.** *Let  $k$  and  $n$  be integers such that  $n \geq k \geq 1$  and let  $m$  be a real number from the closed interval  $[1, k^{1/2}]$ . Let  $A$  be a  $k \times n$   $\{0, 1\}$ -matrix with at least  $mnk^{1/2}$  1-entries. The number of occurrences of  $S$  in  $A$  is at least*

$$\frac{n^2(m^2 - 1)^2}{4} - O(m^3nk^{1/2}).$$

*Proof.* If  $k = 1$ , then  $A$  has at most  $n$  1's and so  $m = 1$  and the claim is trivially satisfied. So we assume that  $k \geq 2$ . We also assume that  $A$  has no empty rows. If  $A$  has empty rows, we remove them and use the claim for the matrix with no empty rows. Since the removal decreases  $k$ , keeps  $n$  the same and increases  $m$ , we obtain the desired estimate.

We first count the number  $q$  of pairs of 1's that are in the same row. Let  $d_i$  be the number of 1's in the  $i$ -th row of  $A$ . We have

$$q = \sum_{\{i: d_i \geq 2\}} \binom{d_i}{2} \geq \sum_{i=1}^k \frac{(d_i - 1)^2}{2}.$$

Let  $d$  be the average number of 1's in a row, that is,

$$d \stackrel{\text{def}}{=} \frac{\sum_{i=1}^k d_i}{k} \geq \frac{mnk^{1/2}}{k} = mnk^{-1/2}.$$

By the convexity of the function  $f(x) = (x - 1)^2/2$ , we have

$$q \geq k \frac{(d - 1)^2}{2} \geq \frac{k}{2} (mnk^{-1/2} - 1)^2 \geq \frac{(mn - k^{1/2})^2}{2} \geq \frac{m^2n^2}{2} - O(mnk^{1/2}).$$

Let  $r_{i,j}$  be the number of rows that have a 1-entry in columns  $i$  and  $j$ . Let  $\mathcal{R}$  be the set of pairs  $\{i, j\}$  of column indices satisfying  $1 \leq i < j \leq n$  and  $r_{i,j} \geq 2$ .

First, we consider the case  $q \leq n^2/2$ . From the estimate  $q \geq (mn - k^{1/2})^2/2$ , we obtain  $m \leq 1 + k^{1/2}/n$ . Therefore  $n^2(m^2 - 1)^2 \in O(k)$  and the result holds trivially, because  $k \leq n$ .

Now, we assume  $q > n^2/2$ , which implies  $|\mathcal{R}| > 0$ . By double counting,

$$q = \sum_{1 \leq i < j \leq n} r_{i,j} \leq \sum_{\{i,j\} \in \mathcal{R}} r_{i,j} + \binom{n}{2} - |\mathcal{R}|.$$

Let

$$r \stackrel{\text{def}}{=} \frac{\sum_{\{i,j\} \in \mathcal{R}} r_{i,j}}{|\mathcal{R}|} \geq \frac{q - (\binom{n}{2} - |\mathcal{R}|)}{|\mathcal{R}|} = \frac{q - \binom{n}{2}}{|\mathcal{R}|} + 1.$$

Let  $s$  be the number of occurrences of  $S$  in  $A$ , that is,  $s = \sum_{\{i,j\} \in \mathcal{R}} \binom{r_{i,j}}{2}$ . By the convexity of  $f(x) = (x-1)^2/2$  and since  $r > 1$ , we have

$$\begin{aligned} s &\geq |\mathcal{R}| \frac{(r-1)^2}{2} \geq \frac{|\mathcal{R}|}{2} \left( \frac{q - \binom{n}{2}}{|\mathcal{R}|} \right)^2 \\ &\geq \frac{(m^2 n^2 / 2 - O(mnk^{1/2}) - n^2 / 2)^2}{2|\mathcal{R}|} \\ &\geq \frac{(n^2(m^2 - 1) - O(mnk^{1/2}))^2}{4n^2} \\ &\geq \frac{n^2(m^2 - 1)^2}{4} - O(m^3 nk^{1/2}). \end{aligned}$$

□

We first give some definitions and outline the proof of the upper bound in Theorem 1.1 without mentioning precise values used. We use a modification of a method of Raz [9], that was used for proving upper bounds in another extremal problem on sets of permutations [9, 2].

A  $k \times n$  *word matrix* is a  $k \times n$  matrix with exactly one 1-entry in every row. A  $k \times n$  *word*  $u$  is a sequence  $u_1, u_2, \dots, u_k$  of  $k$  letters from the alphabet  $[n]$ . The set of  $k \times n$  words and the set of  $k \times n$  word matrices are in the following bijection. The word  $u$  is matched with the matrix  $U$  having 1 on position  $(i, j)$  exactly if  $u_i = j$ . A set  $\mathcal{U}$  of  $k \times n$  word matrices is *reverse-free* if the set of corresponding words is reverse-free.

Given a set  $\mathcal{U}$  of  $k \times n$  word matrices, we let the *overall matrix*  $A_{\mathcal{U}}$  be the  $k \times n$  matrix having 1-entries on those positions where at least one matrix of  $\mathcal{U}$  has a 1-entry. The basic idea is to design a procedure that shrinks the set  $\mathcal{U}$  in order to decrease the number of 1's in the overall matrix. When the overall matrix has few 1's, we use a trivial estimate on the size of what remained in  $\mathcal{U}$ . By analyzing the procedure, we then deduce that the original size of  $\mathcal{U}$  was small.

The shrinking procedure uses the result of Lemma 3.1 applied on the overall matrix. Assume that the overall matrix contains  $S$  on the intersection of rows  $r_1$  and  $r_2$  and columns  $c_1$  and  $c_2$ . Let an *avoided pair* be a pair of 1-entries of the overall matrix that do not appear together in any matrix in  $\mathcal{U}$ . By the reverse-free property of  $\mathcal{U}$ , we know that at least one of the two pairs  $\{(r_1, c_1), (r_2, c_2)\}$  and  $\{(r_1, c_2), (r_2, c_1)\}$  is avoided. When the overall matrix contains many occurrences of  $S$ , we find a 1-entry  $(r, c)$  occurring in many avoided pairs. If the 1-entry  $(r, c)$  is not present in enough matrices from  $\mathcal{U}$ , we remove from  $\mathcal{U}$  all the matrices containing  $(r, c)$ , thus removing  $(r, c)$  from the overall matrix. Otherwise, we keep only the matrices that contain  $(r, c)$ , thus removing all the matrices containing any of the 1-entries that appear in some avoided pair together with  $(r, c)$ .

Given a reverse-free set  $\mathcal{U}$  of  $k \times n$  word matrices, let  $A_{\mathcal{U}}$  be the overall matrix of  $\mathcal{U}$ . Let the *weight*  $|A_{\mathcal{U}}|$  of the overall matrix be the number of its 1-entries. The *density* of the overall matrix is  $m_{\mathcal{U}} = |A_{\mathcal{U}}|/(nk^{1/2})$ . The 1-entry of the overall matrix  $A_{\mathcal{U}}$  on the position  $(r, c)$  is *light* if the number of matrices  $U \in \mathcal{U}$  having 1 on position  $(r, c)$  is at most  $|\mathcal{U}|/n$ . Let the *emptiness*  $z_{\mathcal{U}}$  of  $\mathcal{U}$  be the number of rows of  $A_{\mathcal{U}}$  with at most one 1-entry.

**Observation 3.2.** *Let  $\mathcal{U}$  be a reverse-free set of  $k \times n$  word matrices such that  $A_{\mathcal{U}}$  has a light 1-entry. Then the set  $\mathcal{U}'$  of word matrices of  $\mathcal{U}$  not containing the light 1-entry satisfies*

$$\begin{aligned} |\mathcal{U}'| &\geq \left(1 - \frac{1}{n}\right) |\mathcal{U}|, \\ |A_{\mathcal{U}'}| &\leq |A_{\mathcal{U}}| - 1 \quad \text{and} \\ z_{\mathcal{U}'} &\geq z_{\mathcal{U}}. \end{aligned}$$

Let  $n_0$  be a constant such that for every  $n \geq n_0$ ,  $k \leq n$  and  $m \geq 5$ , every matrix  $A$  with  $mnk^{1/2}$  1's contains  $n^2m^4/3$  occurrences of  $S$ . The existence of  $n_0$  follows from Lemma 3.1.

**Claim 3.3.** *Let  $n \geq n_0$  and let  $k \leq n$ . Let  $\mathcal{U}$  be a reverse-free set of  $k \times n$  word matrices such that  $A_{\mathcal{U}}$  has no light 1-entry and with density  $m_{\mathcal{U}} \geq 5$ . Then there exists a set  $\mathcal{U}' \subset \mathcal{U}$  satisfying*

$$\begin{aligned} |\mathcal{U}'| &\geq \frac{|\mathcal{U}|}{n}, \\ |A_{\mathcal{U}'}| &\leq |A_{\mathcal{U}}| - \frac{2nm_{\mathcal{U}}^3}{3k^{1/2}} \quad \text{and} \\ z_{\mathcal{U}'} &\geq z_{\mathcal{U}} + 1. \end{aligned}$$

*Proof.* The overall matrix  $A_{\mathcal{U}}$  contains  $n^2m_{\mathcal{U}}^4/3$  occurrences of  $S$ . So at least  $n^2m_{\mathcal{U}}^4/3$  pairs of 1-entries of  $A_{\mathcal{U}}$  are avoided. Thus there is a 1-entry of  $A_{\mathcal{U}}$  such that the number of avoided pairs containing this 1-entry is at least

$$\frac{2n^2m_{\mathcal{U}}^4}{3|A_{\mathcal{U}}|} = \frac{2n^2m_{\mathcal{U}}^4}{3nk^{1/2}m_{\mathcal{U}}} = \frac{2nm_{\mathcal{U}}^3}{3k^{1/2}}.$$

Let  $(r, c)$  be the position of this 1-entry. Let  $\mathcal{U}'$  be the set of those matrices from  $\mathcal{U}$  that have 1 at position  $(r, c)$ . We consider a position  $(r', c')$  such that  $\{(r, c), (r', c')\}$  is an avoided pair. Every matrix  $U' \in \mathcal{U}'$  has 0 at position  $(r', c')$ . So also  $A_{\mathcal{U}'}$  has 0 at position  $(r', c')$ . Therefore  $|A_{\mathcal{U}'}| \leq |A_{\mathcal{U}}| - 2nm_{\mathcal{U}}^3/(3k^{1/2})$ . Because  $(r, c)$  is not a light 1-entry,  $|\mathcal{U}'| \geq |\mathcal{U}|/n$ . Since  $\mathcal{U}'$  contains only word matrices, the matrix  $A_{\mathcal{U}'}$  contains only one 1-entry in row  $r$ . On the other hand, the 1-entry at position  $(r, c)$  is contained in at least one occurrence of  $S$  in  $A_{\mathcal{U}}$ , so  $A_{\mathcal{U}}$  contains more than one 1-entry in row  $r$ . Thus  $z_{\mathcal{U}'} \geq z_{\mathcal{U}} + 1$ .  $\square$

**Claim 3.4.** *Let  $\mathcal{U}$  be a set of  $n \times k$  word matrices, where  $n \geq k$ . If  $\mathcal{U}$  is reverse-free, then*

$$|\mathcal{U}| \leq n^k k^{-k/2 + O(k/\log k)}$$

*Proof.* We first consider the case that the density  $m_{\mathcal{U}}$  of the overall matrix is smaller than 10. Since the number of  $k \times n$  word matrices contained in  $A_{\mathcal{U}}$  is maximized when each of its rows has the same number of 1-entries, we obtain

$$|\mathcal{U}| \leq (10nk^{-1/2})^k$$

and the result holds.

Otherwise, we apply the following procedure on  $\mathcal{U}$ . We proceed in several steps. Let  $\mathcal{U}_i \subset \mathcal{U}$  be the set of word matrices before the step  $i$ . Let  $\mathcal{U}_1 = \mathcal{U}$ . If the overall matrix at the beginning of the step  $i$  has a light 1-entry, we obtain  $\mathcal{U}_{i+1}$  from  $\mathcal{U}_i$  by applying Observation 3.2, otherwise, by applying Claim 3.3. Let  $m_i \stackrel{\text{def}}{=} m_{\mathcal{U}_i}$  and  $A_i \stackrel{\text{def}}{=} A_{\mathcal{U}_i}$ . *Light steps* are the steps when Observation 3.2 is applied and *heavy steps* are the remaining ones. The steps are further grouped into *phases*. Phase 1 starts with step  $p_1 = 1$ . For every  $j \geq 2$ , phase  $j$  starts with step  $p_j$  chosen as the smallest index such that  $m_{p_j} \leq m_{p_{j-1}}/2$ . The last phase is the first phase  $\ell$  that decreases the density of the overall matrix below 10. So at the beginning of the last phase, we have

$$m_{p_\ell} \geq 10.$$

Because each light step decreases the number of 1's in the overall matrix by 1, only at most  $nk$  light steps are done during the whole procedure.

It remains to count the heavy steps. At the beginning of a heavy step  $i$  of phase  $j$ , we have

$$m_i \geq m_{p_j}/2.$$

By Claim 3.3, the heavy step decreases the number of 1-entries in the overall matrix by

$$|A_i| - |A_{i+1}| \geq \frac{2nm_i^3}{3k^{1/2}} \geq \frac{nm_{p_j}^3}{12k^{1/2}}.$$

Since the phase  $j$  ends at the moment when at least  $|A_{p_j}|/2$  1-entries are removed, the number of heavy steps of phase  $j$  is at most

$$\left\lceil \frac{nk^{1/2}m_{p_j}/2}{nm_{p_j}^3/(12k^{1/2})} \right\rceil = \left\lceil \frac{6k}{m_{p_j}^2} \right\rceil.$$

Each phase shrinks the weight of the overall matrix by a factor of at least 2, so  $m_{p_j} \geq m_{p_\ell}2^{\ell-j}$  for every  $j$ . We also have for every  $j \in \{1, \dots, \ell\}$

$$10 \leq m_{p_j} \leq k^{1/2}.$$

Let  $t$  be the total number of heavy steps. We have

$$t \leq \sum_{j=1}^{\ell} \left\lceil \frac{6k}{m_{p_j}^2} \right\rceil \leq \sum_{j=1}^{\ell} \frac{7k}{(m_{p_\ell}2^{\ell-j})^2} \leq \frac{7k}{m_{p_\ell}^2} \sum_{j=0}^{\infty} 2^{-2j} \leq \frac{7k}{m_{p_\ell}^2} \frac{4}{3} \leq \frac{k}{10}.$$

Let  $\mathcal{U}'$  be the set of word matrices after phase  $\ell$ . During the whole procedure, at most  $nk$  light steps and  $t \leq k/10$  heavy steps were made. We have

$$|\mathcal{U}'| \geq |\mathcal{U}| \left(1 - \frac{1}{n}\right)^{nk} \left(\frac{1}{n}\right)^t \geq |\mathcal{U}| \frac{1}{e^{2k}} n^{-t}. \quad (3.1)$$

The overall matrix  $A_{\mathcal{U}'}$  has at most  $10nk^{1/2}$  1-entries and at least  $t$  rows with a single 1-entry. The number of  $k \times n$  word matrices contained in  $A_{\mathcal{U}'}$  is maximized when each of its rows with at least 2 1-entries has the same number of 1-entries. Thus,

$$|\mathcal{U}'| \leq \left(\frac{10nk^{1/2}}{k-t}\right)^{k-t} \leq n^{k-t} \left(\frac{12}{k^{1/2}}\right)^k \quad \text{since } t \leq k/10. \quad (3.2)$$



By combining Equations (3.1) and (3.2), we conclude that

$$|\mathcal{U}| \leq n^{k-t} (12k^{-1/2})^k e^{2k} n^t \leq n^k k^{-k/2+O(k/\log k)}.$$

□

## References

- [1] R. C. Baker, G. Harman and J. Pintz, The difference between consecutive primes, II, *Proceedings of The London Mathematical Society* **83** (2001), 532–562.
- [2] J. Cibulka and J. Kynčl, Tight bounds on the maximum size of a set of permutations with bounded VC-dimension, *J. Comb. Theory, Ser. A* **119**(7) (2012), 1461–1478.
- [3] G. P. Egorychev, Proof of the van der Waerden conjecture for permanents, *Siberian Mathematical Journal* **22** (1981), 854–859.
- [4] D. I. Falikman, Proof of the van der Waerden conjecture regarding the permanent of a doubly stochastic matrix, *Mathematical Notes* **29** (1981), 475–479.
- [5] Z. Füredi, On the number of edges of quadrilateral-free graphs, *J. Comb. Theory, Ser. B* **68**(1) (1996), 1–6.
- [6] Z. Füredi and P. Hajnal, Davenport–Schinzel theory of matrices., *Discrete Mathematics* **103**(3) (1992), 233–251.
- [7] Z. Füredi, I. Kantor, A. Monti and B. Sinaimeri, On reverse-free codes and permutations, *SIAM J. Discrete Math.* **24**(3) (2010), 964–978.
- [8] J. Matoušek and J. Nešetřil, *Invitation to Discrete Mathematics*, Oxford University Press (1998), ISBN 0198502079.
- [9] R. Raz, VC-Dimension of Sets of Permutations, *Combinatorica* **20**(2) (2000), 241–255.